

Setting up Single Sign-On using Microsoft SSO for the Cloud Business Fax portal

- Setting up Single Sign-On using Microsoft SSO for the Cloud Business Fax portal 1
- Prerequisites 2
- Cloud Business Fax SSO Setup 2
 - Create a new application 3
 - Choose the tenant 3
 - Register the app 4
- Completing the SSO Integration 7
 - User creation 7
 - Enabling the SSO integration 7
- End user login experience 9

The Cloud Business Fax portal now supports using your business Microsoft account for single sign-on integration. This means once you have enabled SSO for your portal, your users will login using their corporate Microsoft account. Any multifactor authentication you have enabled in your Microsoft domain would also be applied to any user attempting to log into the Cloud Business Fax portal.

This document will provide instructions on the key steps to successfully enabling single sign-on using Microsoft for accessing your Cloud Business Fax portal.

Prerequisites

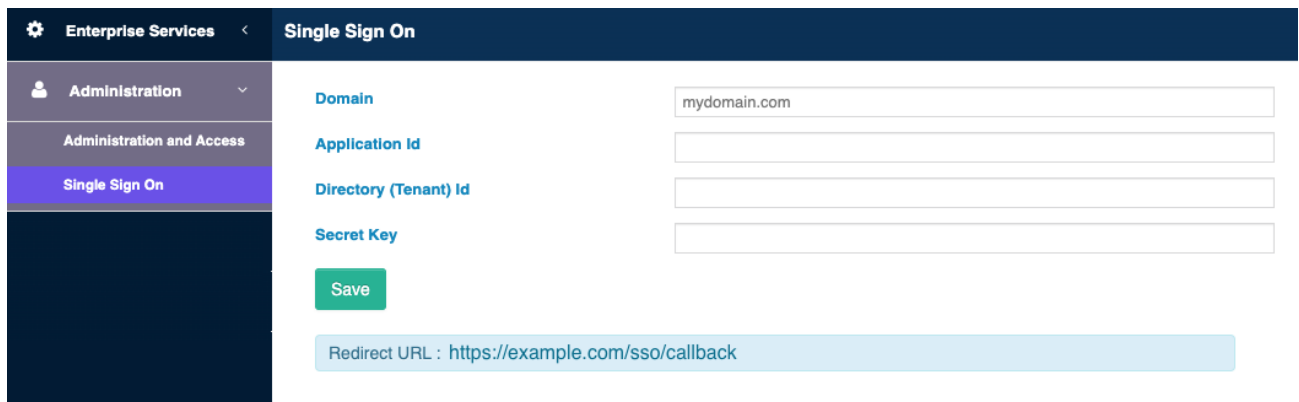
Prior to enabling this feature, there are some things you may want to do if you have existing users on your Cloud Business Fax account. Because logins will change to a user's email address, do the following:

1. Update existing users' email addresses to their corporate Microsoft email address.
2. It's also best to update users' first names/last names to match their Microsoft account data.
3. **NOTE:** If a user has already created a portal login account and is logging in and using the services today, the existing username will be replaced automatically with what is configured for their email address once the single sign-on integration is enabled.
4. Once Single Sign-On is enabled, all user creation will occur once any user enabled for the portal first successfully logs in via their Microsoft account. Users will no longer directly be created in the fax portal.

The steps above can be done in the Administration and Access section in your Cloud Business Fax portal.

Cloud Business Fax SSO Setup

To enable this feature, login to your Cloud Business Fax portal and go to the new Single Sign-On section in Administration.



The screenshot shows the 'Single Sign On' configuration page in the Cloud Business Fax portal. The page has a dark blue header with 'Enterprise Services' and 'Single Sign On'. A left sidebar contains navigation options: 'Administration', 'Administration and Access', and 'Single Sign On' (highlighted in purple). The main content area contains four input fields: 'Domain' (with 'mydomain.com'), 'Application Id', 'Directory (Tenant) Id', and 'Secret Key'. A green 'Save' button is located below the fields. At the bottom, a light blue box displays the 'Redirect URL : https://example.com/sso/callback'.

To use this feature, there are several steps you need to complete in your Microsoft Azure (Encarta) account.

1. Create and register a new application
2. Copy the new Application ID and Directory (Tenant) ID.
3. Set a Redirect URL.
4. Create and copy the Secret Key.
5. Set Assignment Required to control which users can login

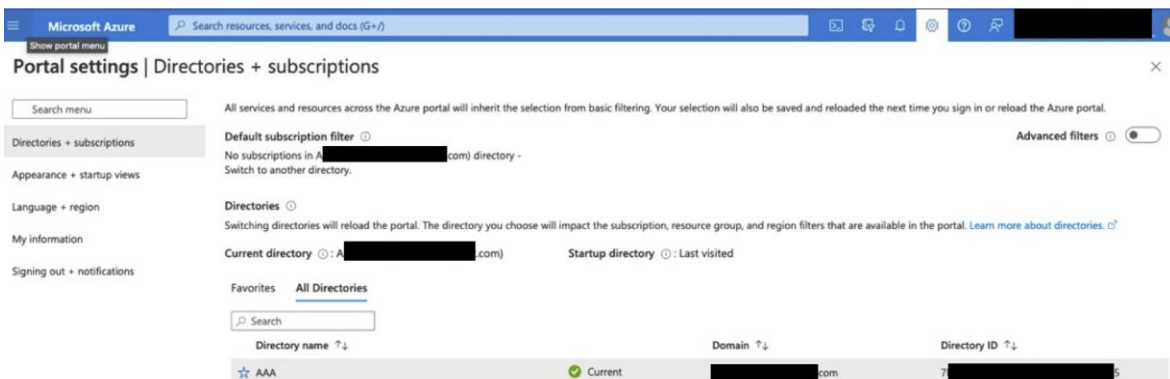
Follow the next sections to complete the setup in Microsoft Azure (Encarta), noting in the above screenshot the fields that you'll need to capture during the process. Do not complete and save the SSO configuration in the Cloud Business Fax portal until you've reviewed the **Completing the SSO Integration** section first.

Create a new application

The first step is to choose the Azure AD tenant where you want to create and configure your application. Complete the following actions.

Choose the tenant

1. Sign in to the Azure (Entra) portal.
2. On the top bar, click on your account, and then on **Switch Directory**.
3. Once the Directory + subscription pane opens, choose the Active Directory tenant where you wish to register your application, from the Favorites or All Directories list.



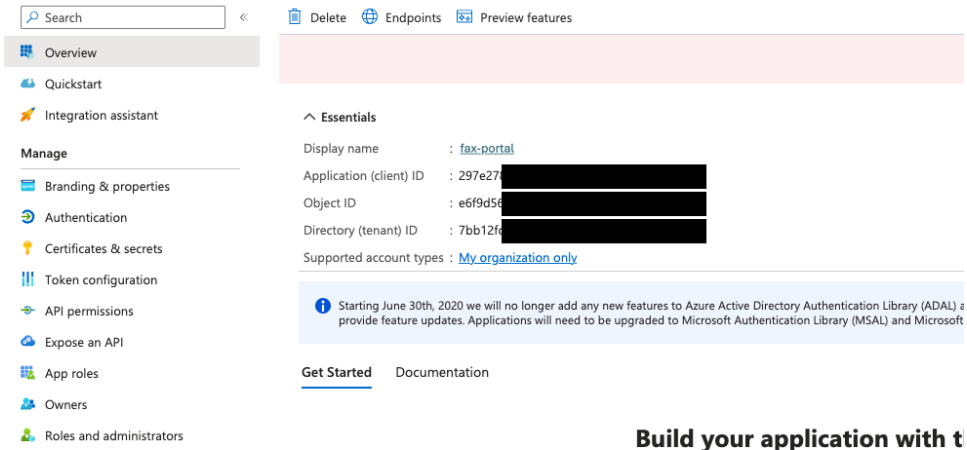
4. Click on **All services** in the portal menu and choose Azure Active Directory.

Register the app

1. In the “Azure Active Directory” pane, click on App registrations and choose New registration.

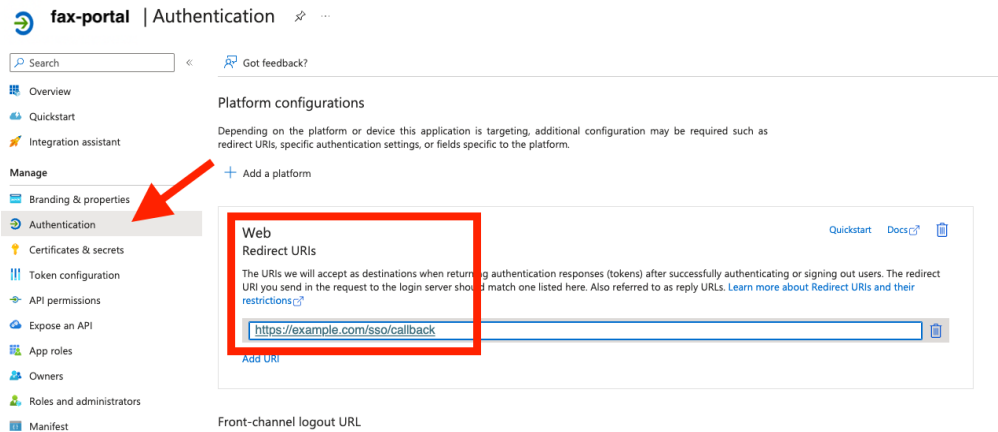
The screenshot shows the Microsoft Entra ID portal interface. On the left, there is a navigation pane with the following items: Overview, Preview features, Diagnose and solve problems, Manage (Users, Groups, External Identities, Roles and administrators, Administrative units, Delegated admin partners, Enterprise applications, Devices, App registrations, Identity Governance). A red arrow points to the 'App registrations' item. The main content area shows the 'AAA | Overview' page for a Microsoft Entra ID tenant. It includes a search bar, tabs for Overview, Monitoring, Properties, Recommendations, and Tutorials, and a 'Basic information' section with fields for Name (AAA), Tenant ID (7b...), Primary domain (...com), License (Microsoft Entra ID P2), and Alerts. A notification banner at the bottom states 'Azure AD is now Microsoft Entra ID'.

2. Enter a friendly name for the application, for example **fax-portal**
3. Click **Register** to register the application.
4. On the application **Overview** page:
 - a. Copy Application (client) ID.
 - b. Copy Directory (tenant) ID.
 - c. Both values will be needed to complete the SSO setup in the Cloud Business Fax portal.



Build your application with t

5. On the application **Authentication** page, under **Redirect URIs**, select **Web**. You will need to enter the Redirect URI shown in your Cloud Business Fax portal in the Single Sign-On page in this field. Do not copy any examples as yours may be different.



6. Click **Save**.
7. On the application menu, choose **Certificates & Secrets** and click on **New client secret** in the Client Secrets section:
 - a. Type a key description (for instance Fax Portal Secret).
 - b. Select a key duration of either **In 1 year**, **In 2 years**, or **Never Expires**.
 - c. The key value will display when you select **Add**. Copy the value to a safe place.

NOTE: This key value will not be displayed again, nor retrievable by any other means, so record it as soon as it is visible from the Azure portal.

- d. You'll need this key later to enable SSO in the Cloud Business Fax portal.

Home > App registrations > **fax-portal** | Certificates & secrets

Overview
Quickstart
Integration assistant

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Add a client secret

Description:

Expires:

8. To control which users have access to the Cloud Business Fax portal, go to the **Properties** page for the new application and set **Assignment required** to **Yes**.

Home > Enterprise applications | All applications > Fax Portal

Fax Portal | Properties
Enterprise Application

Save Discard Delete Got feedback?

Overview
Deployment Plan
Diagnose and solve problems

Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes

Security
Conditional Access
Permissions
Token encryption

Activity
Sign-in logs
Usage & insights
Audit logs
Provisioning logs

View and manage application settings for your organization. Editing prop settings, and user visibility settings requires Global Administrator, Cloud / Administrator roles. [Learn more.](#)

If this application resides in your tenant, you can manage additional prop

Enabled for users to sign-in? Yes No

Name *

Homepage URL

Logo

Application ID

Object ID

Assignment required? Yes No

Visible to users? Yes No

Notes

Completing the SSO Integration

Before completing and saving your SSO integration in the Cloud Business Fax portal, it's important to understand your options for creating users.

User creation

Prior to completing the SSO setup, complete the following steps in the Cloud Business Fax portal:

You can create initial users one of two ways.

1. Using your administrator Cloud Business Fax portal login (before SSO enablement), create the users in the Administration and Access section of the portal. The first name, last name and email address must match how the user is created in Microsoft Azure. You can then assign users to the various fax accounts in your portal in the Enterprise Services section under Cloud Fax. This way, your users are set up with their assigned fax service as soon as they login. **Note that after enablement, user creation occurs automatically when a user first successfully logs in and you can no longer manually create users in the fax portal.**
2. If you don't have existing users in your Cloud Business Fax portal yet, you can defer user creation until after completing the SSO integration. In this method, users are created automatically once the user successfully logs in using their Microsoft account credentials. However, they are not assigned to any fax resources and will not be able to use any of the faxing services. A Cloud Business Fax administrator will need to login to the portal and then assign the user to the correct fax service(s).

Enabling the SSO integration

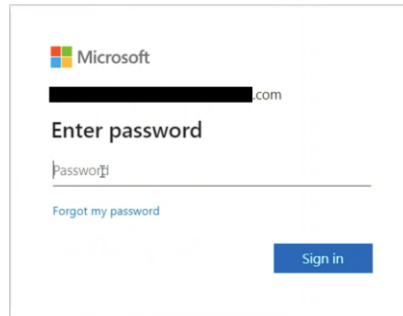
In the Single Sign-On section under Administration in the Cloud Business Fax portal, do the following:

1. First, it's recommended to create a Group Policy in Azure and add the Application ID for the Cloud Business Fax portal to that, then apply that Group Policy only to users needing access to Cloud Business Fax. Do this initially for Administrators of the Cloud Business Fax portal.
2. In the Domain field, enter the domain used for creating the Application ID.
3. In the Application ID field, enter the ID you created above.

4. Enter your Tenant ID in the Directory (Tenant ID) field.
5. Paste the Secret Key you created above for this application in the Secret Key field.
6. Remember to verify the Redirect URL shown on this screen with the one you saved above.
7. **Note that once you click Save to enable the integration, all users logging into your Cloud Business Fax portal account will be required to use their Microsoft account to login, including administrators.**
8. Click **Save** to complete the integration. **Note you will be logged out of the Cloud Business Fax portal as soon as you enable SSO! You will then need to login again, but this time, using your Microsoft account.**
9. Next, apply the Group Policy or add the Application ID to users you want to authorize to use the Cloud Business Fax portal.
10. Let your users know they can login to create their accounts.

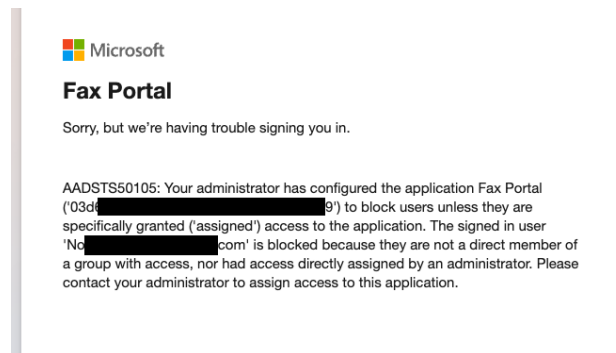
End user login experience

When your users login to the Cloud Business Fax portal, they will be redirected to Microsoft and prompted to enter their email address. The Microsoft login prompt will then ask for their password.

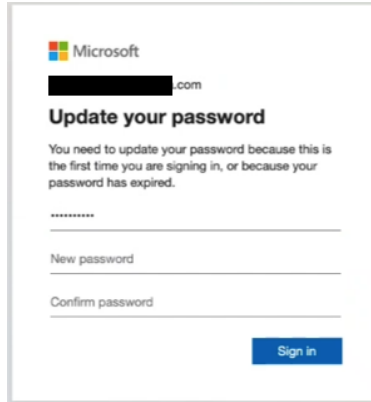


The screenshot shows a Microsoft login interface. At the top left is the Microsoft logo. Below it, the text 'Microsoft' is displayed. A redacted email address is shown as '██████████.com'. The main heading is 'Enter password'. Below this is a password input field with the placeholder text 'Password'. To the left of the input field is a small icon of a person. Below the input field is a link that says 'Forgot my password'. At the bottom right is a blue button labeled 'Sign in'.

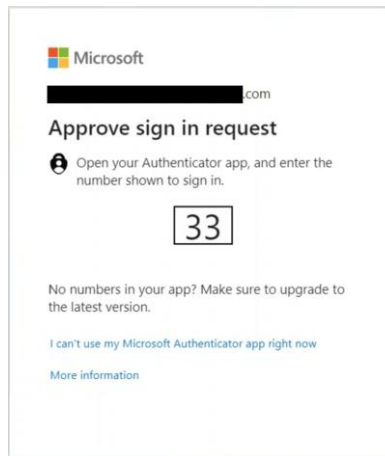
Note that if you have not assigned permissions to a user to allow access to the portal, your end user will see the following error:



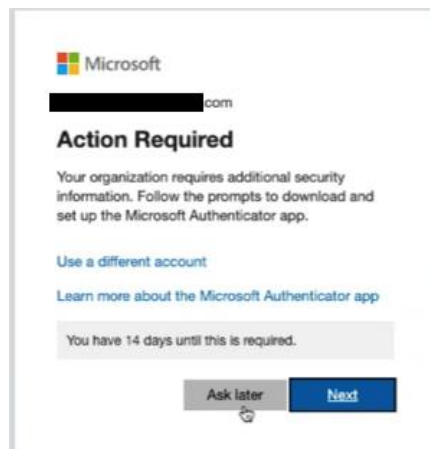
If this is a new account or the password has expired, they may see an Update your password prompt:



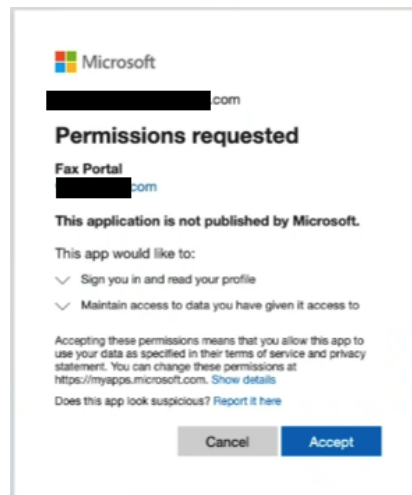
Once updated, this will be followed by any 2FA or MFA options you have configured for your users. If they already have the extra security steps enabled, they will just need to follow their normal method of logging into their Microsoft account, such as using Microsoft Authenticator.



Otherwise, they may be greeted with an Action Required prompt especially if this is a new Microsoft account:



Once the user successfully logs in, they might be greeted with a **Permissions requested** prompt. It's possible that as an Azure Administrator, you may be able to suppress the permissions prompt.



As mentioned in **User creation** above, it's possible the user will get logged in, but have no fax account assigned to them. Have a process in place to allow your users to request being assigned to a fax account. A Cloud Business Fax admin will need to login to complete that account assignment.